OSPF for IPv6 の実装

「*OSPF for IPv6 の実装*」の章では、Open Shortest Path First（OSPF）が拡張され、IPv6 ルーティング プレフィクスのサポートが提供されています。この章では、ネットワークで OSPF for IPv6 を実装するために必要な概念と作業について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「OSPF for IPv6 の実装の機能情報」（P.32）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

OSPF for IPv6 の実装の前提条件

インターフェイスで OSPF for IPv6 をイネーブルにする前に、次の作業を実行する必要があります。

- OSPF ネットワーク方針と IPv6 ネットワークの計画を完了する。たとえば、複数のエリアが必要かどうかを決定する必要があります。
- IPv6 ユニキャスト ルーティングをイネーブルにする。
- インターフェイスで IPv6 をイネーブルにする。
- 認証および暗号化をイネーブルにするために、OSPF for IPv6 に対して IP Security（IPSec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を設定する。

このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。

OSPF for IPv6 の実装の制約事項

- OSPF バージョン 2 for IPv4 および OSPF for IPv6 を使用してデュアルスタック IP ネットワークを実行している場合、OSPF for IPv6 のイネーブル化に使用するコマンドのデフォルトを変更する際は、注意してください。これらのデフォルトを変更すると、OSPF for IPv6 ネットワークに悪影響を及ぼすことがあります。
- 認証は、Cisco IOS Release 12.3(4)T 以降でサポートされています。
- ESP 認証および暗号化は、Cisco IOS Release 12.4(9)T 以降でサポートされています。
- あるルータ上のインターフェイスで見つかった IPv6 アドレスから発信されたパケットは、そのルータ上では拒否されます。

OSPF for IPv6 の実装に関する情報

OSPF for IPv6 の機能

OSPF は、IP 用のルーティング プロトコルです。OSPF は、距離ベクトル型プロトコルではなく、リンクステート型プロトコルです。リンクを、ネットワーキング デバイス上のインターフェイスとして考えます。リンクステート型プロトコルは、送信元マシンと宛先マシンを接続するリンクのステートに基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキング デバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィクス、ネットワーク マスク、接続先のネットワークのタイプ、そのネットワークに接続されているルータなどが含まれます。この情報は、さまざまなタイプの Link-State Advertisement（LSA; リンクステート アドバタイズメント）で伝播されます。

ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。データベースとルーティング テーブルの違いは、データベースには raw データの完全な集まりが含まれるのに対し、ルーティング テーブルには特定のルータ インターフェイス ポートを経由する既知の宛先への最短パスのリストが含まれることです。

（RFC 2740 で説明されている）OSPF バージョン 3 は、IPv6 をサポートしています。

OSPF for IPv6 と OSPF バージョン 2 の比較

OSPF for IPv6 機能のほとんどは、OSPF バージョン 2 の機能と同じです。（RFC 2740 で説明されている）OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

OSPF for IPv6 では、ルーティング プロセスを明示的に作成する必要はありません。インターフェイスで OSPF for IPv6 をイネーブルにすると、ルーティング プロセスおよびそれに関連する設定が作成されます。

OSPF for IPv6 では、インターフェイス コンフィギュレーション モードでコマンドを使用して、各インターフェイスをイネーブルにする必要があります。この機能は、ルータ コンフィギュレーション モードを使用してインターフェイスが間接的にイネーブルになる OSPF バージョン 2 とは異なっています。

OSPF for IPv6 で NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）を使用する場合、ユーザはネイバー リストを使用してルータを手動で設定する必要があります。ネイバー ルータは、それぞれのルータ ID によって識別されます。

IPv6 では、ユーザは 1 つのインターフェイス上に多数のアドレス プレフィクスを設定できます。OSPF for IPv6 には、デフォルトで、1 つのインターフェイス上のすべてのアドレス プレフィクスが組み込まれます。OSPF for IPv6 にインポートするアドレス プレフィクスをユーザが選択することはできません。1 つのインターフェイス上のすべてのアドレス プレフィクスがインポートされるか、1 つのインターフェイス上のいずれのアドレス プレフィクスもインポートされないかのどちらかです。

OSPF バージョン 2 とは異なり、1 つのリンクで OSPF for IPv6 の複数のインスタンスを実行できます。

OSPF for IPv6 では、インターフェイスに IPv4 アドレスを設定しないことが可能です。この場合、ユーザは、OSPF プロセスの開始前に、**router-id** コマンドを使用してルータ ID を設定する必要があります。ルータ ID は、32 ビットの不透明な番号です。OSPF バージョン 2 は、32 ビット IPv4 アドレスを利用して、ルータ ID としての IPv4 アドレスを選択します。インターフェイスで OSPF for IPv6 がイネーブルになっている場合、IPv4 アドレスが存在していると、その IPv4 アドレスがルータ ID として使用されます。複数の IPv4 アドレスが使用可能な場合、OSPF バージョン 2 と同じルールを使用してルータ ID が選択されます。

OSPF では、自動的にループバック インターフェイスが他よりも優先されます。また、すべてのループバック インターフェイスの中で最も高位の IP アドレスが選択されます。ループバック インターフェイスが存在しない場合、ルータ内で最も高位の IP アドレスが選択されます。特定のインターフェイスを使用するように OSPF に指示することはできません。

IPv6 の LSA タイプ

次に、それぞれ用途の異なる LSA タイプを示します。

- ルータ LSA（タイプ 1）：エリアへのルータのリンクのリンク ステートとコストが説明されます。これらの LSA は、エリア内部でだけフラッディングされます。この LSA は、ルータが Area Border Router（ABR; エリア境界ルータ）か Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）か、およびそのルータが仮想リンクの一端であるかどうかを示します。また、タイプ 1 の LSA は、スタブ ネットワークへのアドバタイズにも使用されます。OSPF for IPv6 では、これらの LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。OSPF for IPv6 では、ルータ インターフェイス情報は複数のルータ LSA に分配されます。受信者は、SPF 計算の実行時に、特定のルータから発信されたすべてのルータ LSA を連結する必要があります。
- ネットワーク LSA（タイプ 2）：ネットワークに接続されているすべてのルータのリンクステートおよびコスト情報が説明されます。この LSA は、ネットワーク内のすべてのリンクステートおよびコスト情報を集約したものです。代表ルータだけがこの情報を追跡し、ネットワーク LSA を生成できます。OSPF for IPv6 では、ネットワーク LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。
- ABR のエリア間プレフィクス LSA（タイプ 3）：他のエリア内のルータ（エリア間ルート）に内部ネットワークがアドバタイズされます。タイプ 3 の LSA は、単一のネットワークを表すことも、1 つのアドバタイズメントとして集約された一連のネットワークを表すこともあります。集約 LSA を生成するのは、ABR だけです。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- ASBR のエリア間ルータ LSA（タイプ 4）：ASBR のロケーションがアドバタイズされます。外部ネットワークにアクセスしようとするルータは、これらのアドバタイズメントを使用して、ネクストホップへの最良パスを決定します。タイプ 4 の LSA は、ASBR によって生成されます。
- 自律システム外部 LSA（タイプ 5）：別の AS から（通常は別のルーティング プロトコルから OSPF に）ルートを再分配します。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- リンク LSA（タイプ 8）：ローカルリンク フラッディング スコープを持ちます。関連付けられているリンクを越えてフラッディングされることはありません。リンク LSA は、リンクに接続されている他のすべてのルータに対してルータのリンクローカル アドレスを提供し、リンクに接続されている他のルータに、そのリンクに関連付ける IPv6 プレフィクスのリストを通知します。また、ルータが Options ビットの集まりをアサートして、リンクの起点となるネットワーク LSA と関連付けできるようにします。
- エリア内プレフィクス LSA（タイプ 9）：ルータは、ルータまたは中継ネットワークごとに、それぞれ固有のリンクステート ID を持つ複数のエリア内プレフィクス LSA を発信できます。各エリア内プレフィクス LSA のリンクステート ID は、ルータ LSA またはネットワーク LSA とのアソシエーションを説明するもので、スタブおよび中継ネットワークのプレフィクスを含んでいます。

新しく定義された LSA のほとんどすべてに、アドレス プレフィクスが存在します。プレフィクスは、PrefixLength、PrefixOptions、および Address Prefix の 3 つのフィールドで表現されます。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。タイプ 3 およびタイプ 9 の LSA は、IPv4 ではルータ LSA とネットワーク LSA に含まれているすべての IPv6 プレフィクス情報を伝送します。特定の LSA（ルータ LSA、ネットワーク LSA、エリア間ルータ LSA、およびリンク LSA）の Options フィールドは、OSPF in IPv6 をサポートするために 24 ビットに拡張されました。

OSPF for IPv6 では、エリア間プレフィクス LSA、エリア間ルータ LSA、および自律システム外部 LSA のリンクステート ID の機能は、リンクステート データベースの個々の部分を識別することだけです。OSPF バージョン 2 でリンクステート ID で表されたアドレスまたはルータ ID はすべて、OSPF for IPv6 では LSA の本体で伝送されます。

ネットワーク LSA およびリンク LSA のリンクステート ID は常に、説明されているリンク上の送信元ルータのインターフェイス ID となります。このため、ネットワーク LSA およびリンク LSA は、サイズ制限ができない LSA だけになりました。ネットワーク LSA は、リンクに接続されているすべてのルータをリストする必要があります。リンク LSA は、リンクのルータのアドレス プレフィクスのすべてをリストする必要があります。

OSPF for IPv6 での NBMA

NBMA ネットワークでは、Designated Router（DR; 代表ルータ）または Backup DR（BDR）が LSA フラッディングを実行します。ポイントツーポイントネットワークでは、フラッディングはインターフェイスからネイバーに直接送信されるだけです。

共通セグメントを共有するルータ（2 つのインターフェイス間のレイヤ 2 リンク）は、そのセグメント上でネイバー同士となります。OSPF では、Hello プロトコルを使用して、各インターフェイスから定期的に Hello パケットを送信します。ルータがネイバーの Hello パケット内に自身がリストされていることを認識すると、それらのルータはネイバー同士となります。2 つのルータがネイバーになると、データベースの交換や同期化を行うことができるようになります。これにより、隣接が作成されます。すべてのネイバー ルータが隣接を持っているわけではありません。

ポイントツーポイント ネットワークおよびポイントツーマルチポイント ネットワーク上では、ソフトウェアによってルーティング アップデートがすぐ隣のネイバーにフラッディングされます。DR も BDR もないため、すべてのルーティング情報が各ネットワーキング デバイスにフラッディングされます。

ブロードキャストまたは NBMA セグメントの場合にかぎり、OSPF では、DR と BDR として 1 つずつルータを選択することにより、セグメント上で交換される情報の量を最小限にします。このため、セグメント上の各ルータには、情報交換のための中央接続ポイントがあります。各ルータは、セグメント上の他のルータそれぞれとルーティング アップデートを交換するのではなく、DR および BDR と情報を交換します。DR および BDR は、情報を他のルータに中継します。

ソフトウェアによってセグメント上の各ルータのプライオリティが確認され、DR および BDR となるルータが決定されます。最も高いプライオリティのルータが DR として選択されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。DR が選択されると、BDR が同様の方法で選択されます。プライオリティが 0 に設定されているルータは、DR または BDR になる資格がありません。

OSPF for IPv6 で NBMA を使用する場合、ネイバーを自動的に検出することはできません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。

OSPF for IPv6 での SPF の強制実行

clear ipv6 ospf コマンドとともに **process** キーワードが使用されている場合、OSPF データベースがクリアされて値が再入力されてから、SPF アルゴリズムが実行されます。**clear ipv6 ospf** コマンドとともに **force-spf** キーワードが使用されている場合、SPF アルゴリズムの実行前に OSPF データベースはクリアされません。

高速コンバージェンス - LSA および SPF スロットリング

OSPF for IPv6 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPF でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。また、ミリ秒単位の LSA レート制限を提供することにより、より高速な OSPF コンバージェンスを可能にしています。

以前は、OSPF for IPv6 では、レート制限の SPF 計算および LSA 生成にスタティック タイマーを使用していました。これらのタイマーも設定可能ですが、使用される値を秒単位で指定するため、OSPF for IPv6 コンバージェンスに制約が生まれます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限メカニズムを提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

OSPF for IPv6 でのロード バランシング

ルータは、複数のルーティング プロセス（またはルーティング プロトコル）を介して特定のネットワークへの複数のルートを認識すると、最短の管理ディスタンスを持つルートをルーティング テーブルにインストールします。同じ管理ディスタンスを持つ同じルーティング プロセスを介して認識された多数のルートから、1 つのルートを選択する必要があることもあります。この場合、ルータは宛先へのコスト（またはメトリック）が最小のパスを選択します。各ルーティング プロセスにより、そのコストが別々に計算されます。また、ロード バランシングを実現するために、コストを操作する必要がある場合もあります。

OSPF では、次のようにしてロード バランシングを自動的に実行します。OSPF で複数のインターフェイスを介して宛先に到達できることが確認されたが、各パスのコストが同じである場合、各パスがルーティング テーブルにインストールされます。同じ宛先へのパスの数は、**maximum-paths** コマンドを指定しないかぎり制限されません。デフォルトの最大パスは 16 です。有効範囲は 1 ～ 64 です。

OSPF for IPv6 へのアドレス インポート

OSPF for IPv6 が実行されているインターフェイス上で指定されているアドレス セットを OSPF for IPv6 にインポートするときに、インポートする特定のアドレスをユーザが選択することはできません。すべてのアドレスがインポートされるか、いずれのアドレスもインポートされないかのどちらかです。

OSPF for IPv6 のカスタマイズ

ご使用のネットワークに対して OSPF for IPv6 をカスタマイズすることもできますが、通常はその必要はありません。OSPF in IPv6 のデフォルトは、ほとんどのカスタマーおよび機能の要件を満たすように設定されています。デフォルトを変更する必要がある場合は、IPv6 コマンド リファレンスを参照して、適切な構文を確認してください。

注意 デフォルトを変更する際は、注意してください。デフォルトを変更すると、OSPF for IPv6 ネットワークに悪影響を及ぼすことがあります。

IPsec を使用した OSPF for IPv6 認証サポート

OSPF for IPv6 パケットが変更されてルータに再送信されることにより、ルータが管理者にとって望ましくない動作をすることにならないように、OSPF for IPv6 パケットを認証する必要があります。OSPF for IPv6 では、IP Security（IPSec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して、OSPF for IPv6 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPF for IPv6 では、認証をイネーブルにするために IPsec を使用する必要があります。認証を使用するには、暗号イメージが必要です。これは、OSPF for IPv6 での使用に必要な IPsec API は、暗号イメージにしか含まれていないためです。

OSPF for IPv6 では、認証フィールドが OSPF ヘッダーから削除されています。OSPF が IPv6 上で動作するとき、ルーティング交換の整合性、認証、および機密性を保証するために、OSPF に IPv6 Authentication Header（AH; 認証ヘッダー）または IPv6 ESP ヘッダーが必要となります。IPv6 AH および ESP 拡張ヘッダーを使用すると、OSPF for IPv6 に認証および機密性を提供できます。

IPsec AH を使用するには、**ipv6 ospf authentication** コマンドをイネーブルにする必要があります。IPsec ESP を使用するには、**ipv6 ospf encryption** コマンドをイネーブルにする必要があります。ESP ヘッダーは、単独で適用することも、AH と組み合せて適用することもできます。ESP を使用した場合、暗号化と認証の両方が提供されます。セキュリティ サービスは、通信する 1 組のホスト、通信する 1 組のセキュリティ ゲートウェイ、またはセキュリティ ゲートウェイとホストの間に提供できます。

IPsec を設定するために、ユーザはセキュリティ ポリシーを設定できます。これは、Security Policy Index（SPI）とキーの組み合せです（このキーはハッシュ値の作成および検証に使用されます）。OSPF for IPv6 の IPsec は、インターフェイスまたは OSPF エリアに対して設定できます。セキュリティを強化するには、ユーザは、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。ユーザが OSPF エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。OSPF for IPv6 に対して設定された IPsec は、ユーザには不可視です。

トラフィックを保護するために、アプリケーションによりセキュア ソケット API が使用されます。この API によって、アプリケーションによるセキュア ソケットのオープン、リッスン、およびクローズを許可する必要があります。また、アプリケーションと Secure Socket Layer の間のバインディングにより、Secure Socket Layer は、接続のオープンやイベントのクローズなど、ソケットへの変更をアプリケーションに通知できます。セキュア ソケット API は、ソケットを識別できます。つまり、セキュリティを必要とするトラフィックを伝送するローカルおよびリモートのアドレス、マスク、ポート、およびプロトコルを識別できます。

各インターフェイスのセキュア ソケット ステートは、次のいずれかになります。

- NULL：エリアに対して認証が設定されていれば、インターフェイスに対してセキュア ソケットを作成しません。
- DOWN：インターフェイス（またはインターフェイスが含まれるエリア）に対して IPsec は設定されていますが、OSPF for IPv6 がこのインターフェイスに対するセキュア ソケットの作成を IPsec に要求していないか、またはエラー条件が存在します。
- GOING UP：OSPF for IPv6 は IPsec からのセキュア ソケットを要求したあと、IPsec からの CRYPTO_SS_SOCKET_UP メッセージを待機中です。
- UP：OSPF は、IPsec から CRYPTO_SS_SOCKET_UP メッセージを受信していません。
- CLOSING：インターフェイスのセキュア ソケットはクローズされています。インターフェイスに対して新しいソケットがオープンされることがあります。この場合、現在のセキュア ソケットは DOWN ステートに移行します。オープンされない場合、インターフェイスは UNCONFIGURED となります。
- UNCONFIGURED：インターフェイス上に認証は設定されていません。

OSPF は、DOWN ステートの間、パケットの送信や受け入れを行いません。

IPsec の詳細については、「*IPv6 セキュリティへの IPsec の実装*」を参照してください。

OSPF for IPv6 の仮想リンク

仮想リンクごとに、マスター セキュリティ情報データブロックが作成されます。各インターフェイスでセキュア ソケットをオープンする必要があるため、トランジット エリア内のインターフェイスごとに、対応するセキュリティ情報データブロックが存在することになります。セキュア ソケット ステートは、インターフェイスのセキュリティ情報データブロック内に保持されます。マスター セキュリティ情報データブロック内のステート フィールドは、仮想リンクに対してオープンされたすべてのセキュア ソケットのステータスを反映しています。すべてのセキュア ソケットが UP の場合、仮想リンクのセキュリティ ステートは UP に設定されます。

IPsec が設定された仮想リンク上を送信されるパケットは、事前に決定された送信元アドレスと宛先アドレスを使用する必要があります。エリアのルータのエリア内プレフィクス LSA で見つかった最初のローカル エリア アドレスが、送信元アドレスとして使用されます。この送信元アドレスはエリア データ構造で保存され、セキュア ソケットがオープンされ、パケットが仮想リンク上を送信されるときに使用されます。送信元アドレスが選択されるまで、仮想リンクはポイントツーポイント ステートに移行しません。また、送信元アドレスまたは宛先アドレスが変更された場合は、以前のセキュア ソケットをクローズして、新しいセキュア ソケットをオープンする必要があります。

OSPF コスト計算

コスト コンポーネントは急速に変更される可能性があるため、変更量を抑えてネットワーク全体の変動を小さくする必要があることがあります。S2、S3、および S4 の推奨値は、ネットワークの変更率を抑えるためのネットワーク シミュレーションに基づいています。S1 の推奨値は 0 です。この変数がルート コスト計算から除外されるようにするためです。

全体のリンク コストは、図 1 に示した式を使用して計算されます。

図 1　　全体のリンク コストの式

$$\text{LinkCost} = \text{OC} + \text{BW}\left(\frac{\text{Throughput\_weight}}{100}\right) + \text{Resources}\left(\frac{\text{Resources\_weight}}{100}\right) + \text{Latency}\left(\frac{\text{Latency\_weight}}{100}\right) + \text{L2\_factor}\left(\frac{\text{L2\_weight}}{100}\right)$$

$$\text{OC} = \left[\frac{(\text{ospf\_reference\_bw})}{(\text{MDR})(1000)}\right] \qquad \boxed{\text{ospf\_reference\_bw} = 10 \wedge 8}$$

$$\text{BW} = \frac{(65536)\left(100 - \frac{\text{CDR}}{\text{MDR}}(100)\right)}{100}$$

$$\text{Resources} = \frac{(100 - \text{resources})^3\,(65536)}{1000000}$$

$$\text{Latency} = \text{latency}$$

$$\text{L2\_factor} = \frac{(100 - \text{RLQ})(65536)}{100}$$

231048

表 1 に、OSPF コスト計算で使用される記号を定義します。

表 1　OSPF コスト計算の定義

コスト コンポーネント	コンポーネント定義
OC	デフォルトの OSPF コスト。reference_bw / (MDR*1000)（reference_bw=10^8）を使用して、参照帯域幅から計算されます。
A ～ D	ラジオ固有のデータベースのさまざまな式。0 ～ 64,000 の範囲の結果が生成されます。
A	CDR 関連および MDR 関連の式： (2^16 * (100 – (CDR * 100 / MDR)))/100
B	リソース関連の式： ((100 – RESOURCES)^3 * 2^16 / 10^6)
C	ラジオにより報告される遅延。報告される時点で、すでに 0 ～ 64K の範囲です（LATENCY）。
D	RLF 関連の式： ((100 – RLF) * 2^16)/100
S1 ～ S4	Command-Line Interface（CLI; コマンドライン インターフェイス）からのスカラ重み付け係数入力。これらのスカラは、A ～ D により計算された値を縮小します。 0 の値は、あるコンポーネントに対して 0 ～ 64,000 の全範囲をディセーブルにし、100 の値はイネーブルにします。

各ネットワークに固有の特性があり、実際のネットワーク パフォーマンスを最適化するために異なる設定が必要となることもあるため、これらの推奨値は、OSPFv3 ネットワークを最適化するための開始点として捉えてください。表 2 に、OSPF コスト メトリックの推奨値設定を示します。

表 2　OSPF コスト メトリックの推奨値

設定	メトリックの説明	デフォルト値	推奨値
S1	ipv6 ospf dynamic weight throughout	100	0
S2	ipv6 ospf dynamic weight resources	100	29
S3	ipv6 ospf dynamic weight latency	100	29
S4	ipv6 ospf dynamic weight L2 factor	100	29

次のリストで示すように、この式を使用してデフォルトのパス コストが計算されています。これらの値が使用しているネットワークに適していない場合は、独自のパス コストの計算方法を使用できます。

- 56-kbps シリアル リンク：デフォルトのコストは 1785 です。
- 64-kbps シリアル リンク：デフォルトのコストは 1562 です。
- T1（1.544-Mbps シリアル リンク）：デフォルトのコストは 64 です。
- E1（2.048-Mbps シリアル リンク）：デフォルトのコストは 48 です。
- 4-Mbps トークン リング：デフォルトのコストは 25 です。
- イーサネット：デフォルトのコストは 10 です。
- 16-Mbps トークン リング：デフォルトのコストは 6 です。
- FDDI：デフォルトのコストは 1 です。

- X25：デフォルトのコストは 5208 です。
- 非同期：デフォルトのコストは 10,000 です。
- ATM：デフォルトのコストは 1 です。

これらの設定を示すために、ここでは、VMI インターフェイスに対して OSPF コスト メトリックを定義する例を示します。

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

OSPFv3 グレースフル リスタート

OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。ルータは、再起動モード（グレースフルリスタート対応ルータなど）か、ヘルパー モード（グレースフル リスタート認識ルータなど）のいずれかで、グレースフル リスタートに参加できます。

グレースフル リスタート機能を実行するには、ルータが High Availability（HA; ハイ アベイラビリティ）Stateful Switchover（SSO; ステートフル スイッチオーバー）モード（つまり、デュアル RP）になっている必要があります。グレースフル リスタート機能を備えたルータは、次の場合に、グレースフル リスタート機能を実行します。

- Route Processor（RP; ルート プロセッサ）障害が発生し、スタンバイ RP へのスイッチオーバーが行われた場合
- スタンバイ RP への計画的な RP スイッチオーバーが行われた場合

グレースフル リスタート機能を使用するには、ネイバー ルータがグレースフルリスタート認識ルータであることが必要です。

SSO および Nonstop Forwarding（NSF; ノンストップ フォワーディング）の詳細については、「*Stateful Switchover*」および「*Cisco Nonstop Forwarding*」を参照してください。

BFD での OSPFv3 のサポート

Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）では、OSPFv3 をサポートしています。OSPFv3 に対する BFD の設定方法については、『*Implementing Bidirectional Forwarding Detection for IPv6*』の章を参照してください。

OSPF for IPv6 の実装方法

ここでは、次の各手順について説明します。

- 「インターフェイスでの OSPF for IPv6 のイネーブル化」（P.11）（必須）
- 「OSPF for IPv6 のエリア範囲の定義」（P.11）（任意）
- 「OSPF for IPv6 での IPsec の設定」（P.12）（任意）
- 「OSPF for IPv6 での NBMA インターフェイスの設定」（P.17）（任意）
- 「OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.19）（任意）

- 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）（任意）
- 「SPF 計算の強制実行」（P.23）（任意）
- 「OSPF for IPv6 の設定および動作の確認」（P.23）（任意）

インターフェイスでの OSPF for IPv6 のイネーブル化

ここでは、OSPF for IPv6 をイネーブルにし、各インターフェイスで OSPF for IPv6 を設定する方法について説明します。デフォルトでは、OSPF for IPv6 ルーティングはディセーブルになっており、インターフェイス上に OSPF for IPv6 は設定されていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **例：** `Router(config-if)# ipv6 ospf 1 area 0`	インターフェイスで OSPF for IPv6 をイネーブルにします。

OSPF for IPv6 のエリア範囲の定義

集約されたルートのコストは、集約されるルートの最高コストとなります。たとえば、次のルートが集約されるとします。

```
OI  2001:0DB8:0:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:0DB8:0:8::/64 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:0DB8:0:9::/64 [110/20]
```

```
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

これらは、次のように 1 つの集約されたルートとなります。

```
OI  2001:0DB8::/48 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

ここでは、OSPF エリアのルートを統合または集約する方法について説明します。

前提条件

OSPF for IPv6 ルーティングがイネーブルになっている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*] **例：** `Router(config-rtr)# area 1 range 2001:0DB8::/48`	エリア境界でルートを統合および集約します。

OSPF for IPv6 での IPsec の設定

OSPF for IPv6 の設定を完了し、認証について決定したあとは、グループ内の各ルータでセキュリティ ポリシーを定義する必要があります。セキュリティ ポリシーは、キーと SPI の組み合せで構成されます。セキュリティ ポリシーを定義するには、SPI およびキーを定義する必要があります。

認証ポリシーまたは暗号化ポリシーは、インターフェイスで、または OSPF エリアに対して設定できます。セキュリティ ポリシーは、エリアに対して設定した場合、エリア内のすべてのインターフェイスに適用されます。セキュリティを強化する場合は、各インターフェイスで異なるポリシーを使用してください。

認証および暗号化は、仮想リンク上に設定できます。

ここでは、認証および暗号化を、インターフェイスまたは OSPF エリア、および仮想リンク上に設定する方法について説明します。

- 「インターフェイスでの認証の定義」（P.13）
- 「インターフェイスでの暗号化の定義」（P.14）
- 「OSPF エリア内の認証の定義」（P.15）
- 「OSPF エリア内の暗号化の定義」（P.16）
- 「OSPF エリア内の仮想リンクに対する認証および暗号化の定義」（P.16）

インターフェイスでの認証の定義

ここでは、インターフェイスで認証を定義する方法について説明します。

前提条件

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPF for IPv6 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf authentication ipsec spi** *spi* **md5** [*key-encryption-type* {*key* | **null**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf authentication ipsec spi** *spi* **md5** [*key-encryption-type* {*key* | **null**}] **例：** `Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`	インターフェイスに認証タイプを指定します。

インターフェイスでの暗号化の定義

前提条件

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPF for IPv6 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**} **例：** `Router(config-if) ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D`	インターフェイスに暗号化タイプを指定します。

OSPF エリア内の認証の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	OSPF エリア内の認証をイネーブルにします。

OSPF エリア内の暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 encryption ipsec spi 500 esp null md5 1aaa2bbb3ccc4ddd5eee6fff7aaa8bbb`	OSPF エリア内の暗号化をイネーブルにします。

OSPF エリア内の仮想リンクに対する認証および暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key*
5. **area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi* *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.0.0.1 authentication ipsec spi 940 md5 1234567890ABCDEF1234567890ABCDEF`	OSPF エリア内の仮想リンクに対して認証をイネーブルにします。
ステップ 5	**area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.1.0.1 hello-interval 2 dead-interval 10 encryption ipsec spi 3944 esp null sha1 123456789A123456789B123456789C123456789D`	OSPF エリア内の仮想リンクに対して暗号化をイネーブルにします。

OSPF for IPv6 での NBMA インターフェイスの設定

NBMA インターフェイスを使用するようにネットワーク内の OSPF for IPv6 をカスタマイズできます。OSPF for IPv6 は、NBMA インターフェイスを介してネイバーを自動的に検出することはできません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。ここでは、NBMA インターフェイスの設定方法について説明します。

前提条件

NBMA インターフェイスを設定する前に、次の作業を実行する必要があります。

- ネットワークを NBMA ネットワークとして設定する。
- 各ネイバーを識別する。

制約事項

- NBMA インターフェイスの使用時に、ネイバーを自動的に検出することはできません。NBMA インターフェイスの使用時には、ネイバーを検出するようにルータを手動で設定する必要があります。
- **ipv6 ospf neighbor** コマンドを設定するときに使用する IPv6 アドレスは、ネイバーのリンクローカル アドレスにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. **ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface serial 0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **例：** `Router(config-if)#  frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120`	宛先アドレスへの接続に使用する宛先 IPv6 アドレスと Data-Link Connection Identifier（DLCI; データリンク接続識別子）との間のマッピングを定義します。 • この例では、NBMA リンクはフレーム リレーです。他の種類の NBMA リンクに対しては、別のマッピング コマンドを使用します。
ステップ 5	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **例：** `Router(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	OSPF for IPv6 ネイバー ルータを設定します。

OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa** *start-interval hold-interval max-interval*
6. **timers lsa arrival** *milliseconds*
7. **timers pacing flood** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **例：** `Router(config-rtr)# timers throttle spf 200 200 200`	SPF スロットリングをオンにします。
ステップ 5	**timers throttle lsa** *start-interval hold-interval max-interval* **例：** `Router(config-rtr)# timers throttle lsa 300 300 300`	OSPF for IPv6 の LSA 生成に対してレート制限値を設定します。

	コマンドまたはアクション	目的
ステップ 6	**timers lsa arrival** *milliseconds* **例：** `Router(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPF ネイバーから同じ LSA を受信する最小間隔を設定します。
ステップ 7	**timers pacing flood** *milliseconds* **例：** `Router(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。

LSA および SPF レート制限に対するイベント ロギングのイネーブル化

OSPF for IPv6 イベント ログは、OSPF for IPv6 インスタンスごとに保持されます。ここでは、LSA および SPF レート制限機能に対してイベント ロギングをイネーブルにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **event-log** [**size** [*number of events*]] [**one-shot**] [**pause**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**event-log** [**size** [*number of events*]] [**one-shot**] [**pause**] **例：** `Router(config-rtr)# event-log size 10000 one-shot`	イベント ロギングをイネーブルにします。

イベント ログの内容のクリア

手順の概要

1. **enable**
2. **clear ipv6 ospf** [*process-id*] **events**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 ospf** [*process-id*] **events** **例：** `Router# clear ipv6 ospf 1 events`	OSPF ルーティング プロセス ID に基づいて、OSPF for IPv6 イベント ログの内容をクリアします。

OSPFv3 グレースフル リスタートのイネーブル化

グレースフル リスタート機能は、グレースフルリスタート対応ルータおよびグレースフルリスタート認識ルータに対してイネーブルにできます。ここでは、OSPFv3 グレースフル リスタートをイネーブルにする方法について説明します。

- 「グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
- 「グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.22）

グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart** [**restart-interval** *interval*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart** [**restart-interval** *interval*] **例：** `Router(config-rtr)# graceful-restart`	グレースフルリスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart helper** {**disable** | **strict-lsa-checking**} **例：** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフルリスタート認識ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

SPF 計算の強制実行

手順の概要

1. **enable**
2. **clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**}

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} **例：** `Router# clear ipv6 ospf force-spf`	OSPF ルーティング プロセス ID に基づいて OSPF ステートをクリアし、SPF アルゴリズムを強制的に開始します。

OSPF for IPv6 の設定および動作の確認

手順の概要

1. **enable**
2. **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*]
3. **show ipv6 ospf** [*process-id*] [*area-id*]
4. **show crypto ipsec policy** [**name** *policy-name*]
5. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**]
6. **show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*] **例：** `Router# show ipv6 ospf interface`	OSPF 関連のインターフェイス情報を表示します。
ステップ 3	**show ipv6 ospf** [*process-id*] [*area-id*] **例：** `Router# show ipv6 ospf`	OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 4	**show crypto ipsec policy** [**name** *policy-name*] **例：** `Router# show crypto ipsec policy`	各 IPsec パラメータのパラメータを表示します。
ステップ 5	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**] **例：** `Router# show crypto ipsec sa ipv6`	現在の Security Association（SA; セキュリティ アソシエーション）によって使用されている設定を表示します。
ステップ 6	**show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **例：** `Router# show ipv6 ospf event spf`	OSPF for IPv6 イベントに関する詳細情報を表示します。

例

show ipv6 ospf interface コマンドの出力例

次に、暗号化および認証によって保護された通常のインターフェイスおよび仮想リンクを使用した、**show ipv6 ospf interface** コマンドの出力例を示します。

```
Router# show ipv6 ospf interface

OSPFv3_VL1 is up, line protocol is up
   Interface ID 69
```

```
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 64
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Hello due in 00:00:00
   Index 1/3/5, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 1
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
OSPFv3_VL0 is up, line protocol is up
   Interface ID 67
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 128
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/4, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 10
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.1.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
Ethernet1/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6601, Interface ID 6
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type BROADCAST, Cost: 10
   Transmit Delay is 1 sec, State DR, Priority 1
   Designated Router (ID) 10.0.0.1, local address FE80::A8BB:CCFF:FE00:6601
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/1, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
Serial12/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 50
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   AES-CBC encryption SHA-1 auth SPI 2503, secure socket UP (errors: 0)
   authentication NULL
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1
```

```
   Suppress hello for 0 neighbor(s)
Serial11/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 46
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   MD5 authentication (Area) SPI 500, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/2, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.0.0.1
   Suppress hello for 0 neighbor(s)
```

show ipv6 ospf コマンドの出力例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 172.16.3.3
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x218D
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Area 1
        Number of interfaces in this area is 2
        SPF algorithm executed 9 times
        Number of LSA 15. Checksum Sum 0x67581
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show crypto ipsec policy コマンドの出力例

次に、**show crypto ipsec policy** コマンドの出力例を示します。

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:     OSPFv3-1-1000
Policy refcount: 1
Inbound  AH SPI: 1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound  AH Key: 1234567890ABCDEF1234567890ABCDEF
Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF
Transform set:   ah-md5-hmac
```

show crypto ipsec sa ipv6 コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show crypto ipsec sa ipv6
```

```
IPv6 IPsec SA info for interface Ethernet0/0

   protected policy name:OSPFv3-1-1000
   IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

   local  ident (addr/prefixlen/proto/port):(FE80::/10/89/0)
   remote ident (addr/prefixlen/proto/port):(::/0/89/0)
   current_peer:::
     PERMIT, flags={origin_is_acl,}
    #pkts encaps:21, #pkts encrypt:0, #pkts digest:21
    #pkts decaps:20, #pkts decrypt:0, #pkts verify:20
    #pkts compressed:0, #pkts decompressed:0
    #pkts not compressed:0, #pkts compr. failed:0
    #pkts not decompressed:0, #pkts decompress failed:0
    #send errors 0, #recv errors 0

    local crypto endpt. ::, remote crypto endpt. ::
    path mtu 1500, media mtu 1500
    current outbound spi:0x3E8(1000)

     inbound ESP SAs:

     inbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2000, flow_id:1, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     inbound PCP SAs:

     outbound ESP SAs:

     outbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2001, flow_id:2, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     outbound PCP SAs:
```

show ipv6 ospf graceful-restart コマンドの出力例

次に、**show ipv6 ospf graceful-restart** コマンドの出力例を示します。

```
Router# show ipv6 ospf graceful-restart

Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

OSPF for IPv6 を実装するための設定例

例：インターフェイス設定での OSPF for IPv6 のイネーブル化

次に、OSPF ルーティング プロセス 109 をインターフェイス上で動作するように設定し、エリア 1 に配置する例を示します。

```
ipv6 ospf 109 area 1
```

例：OSPF for IPv6 のエリア範囲の定義

次に、OSPF for IPv6 のエリア範囲を指定する例を示します。

```
interface Ethernet7/0
 ipv6 address 2001:0DB8:0:7::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet8/0
 ipv6 address 2001:0DB8:0:8::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet9/0
 ipv6 address 2001:0DB8:0:9::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 router-id 10.11.11.1
 area 1 range 2001:0DB8::/48
```

例：インターフェイスでの認証の定義

次に、イーサネット 0/0 インターフェイスで認証を定義する例を示します。

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF

interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

例：OSPF エリア内の認証の定義

次に、OSPF エリア 0 で認証を定義する例を示します。

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

例：NBMA インターフェイスの設定

次に、Ipv6 アドレスが FE80::A8BB:CCFF:FE00:C01 の OSPF ネイバー ルータを設定する例を示します。

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C0
```

例：OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定

次に、SPF および LSA スロットル タイマーの設定値を表示する例を示します。

```
Router# show ipv6 ospf

 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

例：SPF 設定の強制実行

次に、SPF をトリガーして、SPF を再実行し、ルーティング テーブルに値を再入力する例を示します。

```
clear ipv6 ospf force-spf
```

その他の関連資料

関連資料

関連項目	参照先
OSPF でのルータ ID の設定	• 『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring OSPF」 • 『*Cisco IOS IP Routing Protocols Command Reference*』
OSPF for IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
基本的な IPv6 接続の実装	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPsec for IPv6	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec for IPv6 Security」
OSPFv3 に対する BFD サポート	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Bidirectional Forwarding Detection for IPv6」
ステートフル スイッチオーバー	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」
Cisco ノンストップ フォワーディング	『*Cisco* IOS High Availability Configuration Guide』の「Cisco Nonstop Forwarding」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-IETF-IP-FORWARD-MIB • CISCO-IETF-IP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2740	『*OSPF for IPv6*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 5187	『*OSPFv3 Graceful Restart*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

OSPF for IPv6 の実装の機能情報

表 3 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 3　OSPF for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：OSPF for IPv6（OSPFv3）	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)M 15.0(1)S	OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。 このマニュアルでは、この機能について説明しています。
IPv6 ルーティング：OSPF for IPv6 での LSA タイプ	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 の機能」（P.3） • 「IPv6 の LSA タイプ」（P.4）

表 3　OSPF for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：高速コンバージェンス - LSA および SPF スロットリング	12.2(33)SB 12.2(33)SRC 12.2(33)XNE 15.0(1)M	OSPF for IPv6 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPF でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「高速コンバージェンス - LSA および SPF スロットリング」（P.6） • 「OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.19） • 「LSA および SPF レート制限に対するイベント ロギングのイネーブル化」（P.20） • 「イベント ログの内容のクリア」（P.21） • 「例：OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.29）
IPv6 ルーティング：OSPF for IPv6 での NBMA インターフェイス	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	NBMA ネットワークでは、DR またはバックアップ DR が LSA フラッディングを実行します。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 での NBMA」（P.5） • 「OSPF for IPv6 での NBMA インターフェイスの設定」（P.17）
IPv6 ルーティング：OSPF for IPv6 での SPF の強制実行	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	この機能により、OSPF データベースのクリアおよび再入力が可能になります。そのあとで、SPF アルゴリズムが実行されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 での SPF の強制実行」（P.5） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
IPv6 ルーティング：OSPF for IPv6 でのロード バランシング	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	OSPF for IPv6 では、自動的にロード バランシングが実行されます。 この機能に関する詳細については、次の項を参照してください。 • 「OSPF for IPv6 でのロード バランシング」（P.6）

表 3　OSPF for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 の認証サポート	12.3(4)T 12.4 12.4(2)T	OSPF for IPv6 では、IPsec セキュア ソケット API を使用して、OSPF for IPv6 パケットに認証を追加しています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPsec を使用した OSPF for IPv6 認証サポート」（P.7） • 「OSPF for IPv6 での IPsec の設定」（P.12） • 「インターフェイスでの認証の定義」（P.13） • 「OSPF エリア内の認証の定義」（P.15）
IPv6 ルーティング：OSPF IPv6（OSPFv3）IPsec ESP 暗号化および認証	12.4(9)T	IPv6 ESP 拡張ヘッダーを使用すると、OSPF for IPv6 に認証および機密性を提供できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 の実装の制約事項」（P.2） • 「IPsec を使用した OSPF for IPv6 認証サポート」（P.7） • 「インターフェイスでの暗号化の定義」（P.14） • 「OSPF エリア内の暗号化の定義」（P.16） • 「OSPF エリア内の仮想リンクに対する認証および暗号化の定義」（P.16）
OSPFv3 ダイナミック インターフェイス コスト サポート	12.4(15)T	OSPFv3 ダイナミック インターフェイス コスト サポートでは、OSPF for IPv6 コスト メトリックを拡張して、Mobile Ad Hoc Networking のサポートを提供しています。 この機能に関する詳細については、次の項を参照してください。 • 「OSPF コスト計算」（P.8）
OSPFv3 グレースフル リスタート	12.2(33)SRE 12.2(33)XNE 15.0(1)M	OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 グレースフル リスタート」（P.10） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
OSPFv3 for BFD	12.2(33)SRE 15.0(1)S 15.1(2)T	BFD は、ダイナミック ルーティング プロトコル OSPF for IPv6（OSPFv3）をサポートしています。 この機能に関する詳細については、次の項を参照してください。 • 「BFD での OSPFv3 のサポート」（P.10）